

Quantum gambling based on Nash-equilibrium

Pei Zhang,^{1,2} Xiao-Qi Zhou,^{2,*} Yun-Long Wang,¹ Peter J. Shadbolt,²
Yong-Sheng Zhang,³ Hong Gao,¹ Fu-Li Li,¹ and Jeremy L. O'Brien²

¹*MOE Key Laboratory for Nonequilibrium Synthesis and Modulation of Condensed Matter,
Department of Applied Physics, Xi'an Jiaotong University, Xi'an 710049, China*

²*Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering,
University of Bristol, BS8 1UB, United Kingdom*

³*Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, China*

A fair gambling is hard to be made between two spatially separated parties without introducing a trusted third party. Here we propose a novel gambling protocol, which enables fair gambling between two distant parties without the help of a third party. By incorporating the key concepts and methods of game theory, our protocol will force the two parties to move their strategies to a Nash-equilibrium point which guarantees the fairness through the physical laws of quantum mechanics. Furthermore, we show that our protocol can be easily adapted to a biased version, which would find applications in lottery, casino, etc. A proof-of-principle optical demonstration of this protocol is reported as well.

PACS numbers: 02.50.Le, 03.67.-a, 42.50.Ex

Gambling—a game in which people wager money or something valuable on an event with an uncertain outcome—has a wide range of applications in every aspects of human society [1]. However, despite its long history and wide spread usages, it has a long standing problem yet to be resolved. Suppose a gambler (say Bob) wants to gamble with the Casino (say Alice), how does Bob know the gambling machine (GM) provided by Alice is not biased towards Alice herself, especially in the case of online gambling or lotteries?

The standard solution to this problem is to introduce a trusted third party to provide an unbiased GM to make sure the gambling is fair to both parties. However, in some cases such third party which is trusted by both parties does not exist. Surprisingly, by drawing from the classical [2] and quantum game theory [3, 4], we have found a protocol which enables two parties to create an unbiased GM themselves to perform a fair gambling without introducing any third party. The GM, which has two independent parameters, is constructed by Alice and Bob together who can change the values of the two parameters respectively. Furthermore, the GM is elaborately designed in a way that a Nash-equilibrium [2] exists—each party has a strategy to choose his/her parameter which can guarantee his/her gain is no less than a certain amount and neither of the two parties can benefit from changing his/her own parameter unilaterally. In this way, Alice and Bob are ‘forced’ to choose the Nash-equilibrium in their own favor so that a stable GM can be established.

The paper is structured as follows. First, we will describe the protocol in detail and explain how the Nash-equilibrium can guarantee the GM to be unbiased to each party. Then, we will show how to generalize this protocol to a full family of quantum gambling, including both biased and unbiased, by introducing several parameters. At last, we present a proof-of-principle optical experi-

ment to demonstrate the protocol.

The rules of the game and the strategies the players should follow are explained below.

The rules of the game: Alice has two boxes, named A and B , which are used to store a particle. The quantum states of the particle stored in the two boxes are denoted $|a\rangle$ and $|b\rangle$, respectively. Alice prepares the particle in a state and then sends the box B to Bob. Bob wins in one of the following cases: (1) Bob opens the box B and find the particle. (2) Bob does not find the particle in box B and asks Alice to send him the box A . Bob then detects the state Alice prepared is different from the committed state $|\psi_c\rangle$, where $|\psi_c\rangle = \frac{1}{3}|a\rangle + \frac{2\sqrt{2}}{3}|b\rangle$. In any other cases, Alice wins.

Alice’s strategy: Alice prepares the particle in the following state:

$$|\psi\rangle = \sqrt{1-\alpha}|a\rangle + \sqrt{\alpha}|b\rangle, \quad (1)$$

where α is a parameter controlled by Alice ($0 \leq \alpha \leq 1$).

Bob’s strategy:

After receiving the box B , Bob splits the particle into two parts. One part is still stored in box B and the other part is stored in a new box B' . Specifically, Bob performs the following operation: Bob splits the box into two parts, B and B' :

$$|b\rangle \longrightarrow \sqrt{1-\beta}|b\rangle + \sqrt{\beta}|b'\rangle, \quad (2)$$

where $|b'\rangle$ denotes the quantum state of the particle stored in the box B' . The splitting ratio β is a parameter controlled by Bob ($0 \leq \beta \leq 1$). After the splitting, Bob opens the box B and measures the projection operator on the state $|b\rangle$. If he finds the particle in the box B , he wins. If he doesn’t, he asks Alice for the box A and combines it with the box B' to make a verification. If the verification shows the initial state Alice prepared is

different from the committed state $|\psi_c\rangle$, Bob still wins; otherwise, Alice wins.

This completes the definition of our protocol.

Let us briefly analyze the protocol and both players' strategies. For Alice, she has a motivation to prepare a state that the particle has a higher chance to stay in box A (choosing a small α), so that Bob has a lower chance to find the particle in box B . However, if α is too small, the discrepancy between the prepared and the committed state would be too big which will result in a higher chance for Alice to lose in the verification stage—there is a tradeoff for Alice to choose her strategy (parameter α). Similar analysis can apply to Bob's strategy as well. Bob can't rely solely on the $|b\rangle$ projection stage (choosing a small β) or the verification stage (choosing a big β). He needs to consider both stages and choose an intermediate β to maximize his chance to win. By now, the analysis is just qualitative. Actually we have found that there exists best strategies for both parties—the best strategy for Alice (Bob) is to set $\alpha = \frac{1}{3}$ ($\beta = \frac{1}{4}$). The average gain of Alice (Bob) G_a (G_b) will never be negative once she (he) chooses α (β) to be $\frac{1}{3}$ ($\frac{1}{4}$), where the equation $G_a + G_b = 0$ holds as the gambling is a zero-sum game. When both of them choose their best strategies, G_a and G_b have to be zero and a fair gambling will be achieved.

To prove the above claims and features of the protocol, let us write down the expression for G_b first [5],

$$G_b = P_1 + P_2 - (1 - P_1 - P_2), \quad (3)$$

where P_1 and P_2 denote the probability for Bob to find the particle in box B and to find the initial state is different with committed state, respectively. When Bob receives the box B and splits one part to the box B' , the state becomes

$$|\psi_0\rangle = \sqrt{1-\alpha}|a\rangle + \sqrt{\alpha}(\sqrt{1-\beta}|b\rangle + \sqrt{\beta}|b'\rangle). \quad (4)$$

From Eq. 4, it is straightforward to calculate the probability (P_1) of finding the particle in box B ,

$$P_1 = \|\langle b|\psi_0\rangle\|^2 = \alpha(1-\beta). \quad (5)$$

The state of the particle will collapse to $|\psi'_0\rangle$ if Bob fails to detect the particle in box B , where

$$|\psi'_0\rangle = \sqrt{\frac{1-\alpha}{1-\alpha+\beta\alpha}}|a\rangle + \sqrt{\frac{\beta\alpha}{1-\alpha+\beta\alpha}}|b'\rangle, \quad (6)$$

If Alice did prepare the particle in the committed state $|\psi_c\rangle$ initially, the state at this stage will be $|\psi'_c\rangle$

$$|\psi'_c\rangle = \sqrt{\frac{1}{1+8\beta}}|a\rangle + \sqrt{\frac{8\beta}{1+8\beta}}|b'\rangle. \quad (7)$$

Bob then makes a projection measurement on $|\psi'_c\rangle$ for the verification. If the outcome is negative, Bob knows

with certainty that state Alice prepared is different with the committed state $|\psi_c\rangle$. The probability of detecting such event is given by

$$\begin{aligned} P_2 &= (1 - P_1)(1 - \|\langle\psi'_c|\psi'_0\rangle\|^2) \\ &= \frac{\beta[8 - 7\alpha - 4\sqrt{2\alpha(1-\alpha)}]}{1 + 8\beta} \end{aligned} \quad (8)$$

By substituting Eqs. (5) and (8) into Eq. (3), we can get G_b as a function of α and β :

$$\begin{aligned} G_b(\alpha, \beta) &= \frac{1}{1+8\beta} \{2\alpha + 8\beta - 1 \\ &\quad - 8[2\beta^2\alpha - \beta\sqrt{2\alpha(1-\alpha)}]\}. \end{aligned} \quad (9)$$

As shown in Fig. 1a, the G_b function is saddle-shaped and the saddle point is at $\alpha = \frac{1}{3}$ and $\beta = \frac{1}{4}$. Figures 1b and 1c are the projection of the G_b function to the $\beta - G_b$ plane and $\alpha - G_a$ plane, respectively. From Fig. 1b (1c), it's clear that, no matter what strategy Alice (Bob) chooses, Bob's (Alice's) gain will always be non-negative if he (she) sets his (her) parameter to be $\frac{1}{4}$ ($\frac{1}{3}$). Any party changes his/her strategy unilaterally will only decrease his/her own gain. In this way, Nash-equilibrium is achieved and both parties will stick their strategy and thus a stable and fair game is achieved.

The above scheme effectively realizes a coin-tossing protocol [6–13] where the one-shot gains for both parties are balanced and the expectation value of the gains for both parties are zero. However, in practice, there are much more diverse gambling protocols, such as Roulette or Lottery, where the one-shot gains are unbalanced and the expectation value of the gains are non-zero. As only the ratio of the one-shot gains matters, without loss of generality, we fix Alice's one-shot gain to be 1 and Bob's one-shot gain to be R . Now the task is to design a stable gambling protocol in which Bob's one-shot gain is R and the expectation value of Bob's gain G_b to be δ . It can be proved that our scheme can be easily extended to realize such gambling protocol by just reappointing the committed state to be

$$|\psi_c\rangle = \sqrt{1-\gamma}|a\rangle + \sqrt{\gamma}|b\rangle, \quad (10)$$

where

$$\gamma = \frac{4(1+\delta)(1+R)}{(2+\delta+R)^2}. \quad (11)$$

The Nash-equilibrium point for Alice's and Bob's strategies would be $\alpha = \frac{1-\sqrt{1-\gamma}}{2}$ and $\beta = \frac{-1+\gamma+\sqrt{1-\gamma}}{\gamma}$. Following similar reasoning shown in last paragraph, setting α and β to the above values are the best strategies for Alice and Bob, as none of them can benefit from changing their own strategy unilaterally. The earlier protocol can be regarded as a special case where $R = 1$, $\delta = 0$ and $\gamma = 8/9$. The detailed calculation and proof can be found in the Appendix.

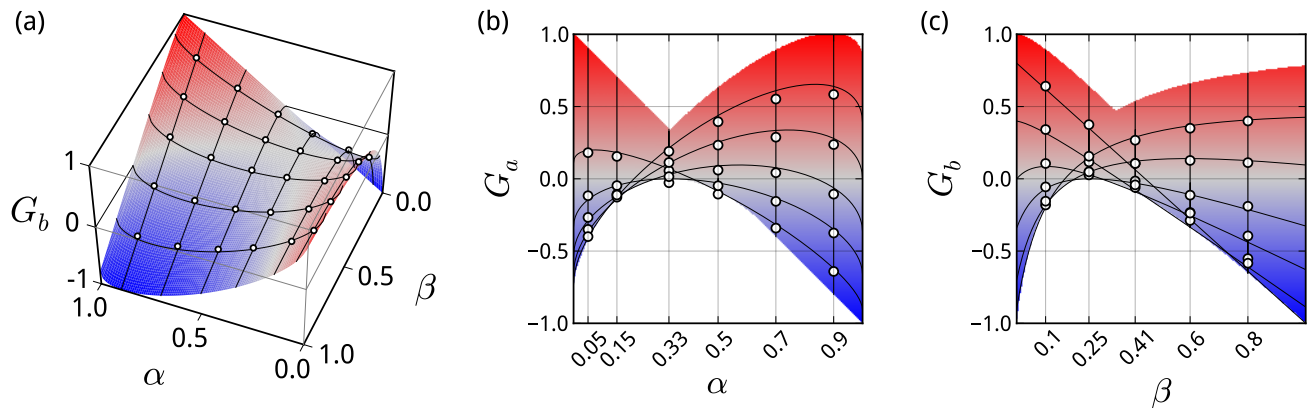


FIG. 1. Theoretical (surface) and experimental (circles) results of our protocol under $R = 1$ and $\gamma = 8/9$. (a) Bob's average gain in a three dimensional view. The Nash-equilibrium is the point of $G_b = 0$, $\beta = 1/4$ and $\alpha = 1/3$. (b) Bob's gain under his parameter β . The best strategy is choosing $\beta = 1/4$. (c) Alice's gain under her parameter α . Her best choice is $\alpha = 1/3$.

Besides proposing the theory, we also implemented a proof-of-principle experiment to demonstrate our gambling protocols. As shown in Fig. 2, a He-Ne laser centred at 632.8 nm is attenuated to the level of ~ 100 KHz count rate to serve as single-photon source. The two polarization states $|V\rangle$ and $|H\rangle$ are encoded as the two box states $|a\rangle$ and $|b\rangle$, respectively. Thus the two parameters α and β can be easily managed by half-wave-plates (HWP). HWP₁ is controlled by Alice to prepare the state $|\psi\rangle$. Bob uses HWP₂ and polarized beam splitter (PBS₂) to split the state $|b\rangle$ to $|b\rangle$ and $|b'\rangle$, and measures P_1 at the single-photon detector (D₁). Then $|b'\rangle$ and $|a\rangle$ are combined at PBS₁ for verification.

A Sagnac interferometer (with interference visibility of 96%) is used in our setup to make sure the phase stability is maintained throughout the whole experiment. HWP₃ and PBS₃ are used for the projective measurement, where P_2 and P_3 can be measured from D₂ and D₃, respectively.

In our experiment, we simulated a fair coin-tossing GM, where R and γ are set to be 1 and $8/9$, respectively. Both Alice and Bob chose a series of strategies and the final gains for both parties are measured and recorded. The results are shown in Fig. 1. All the data are well agreed with the theoretical predictions. From the results, we can clearly see that the best gain Alice (Bob) can get is when she (he) choose the strategy $\alpha = 1/3$ ($\beta = 1/4$). For their own good, Alice and Bob would both choose their best strategies and thus a Nash-equilibrium is formed and a fair gamble is achieved.

The errors of our experimental results mainly come from the imperfection of components used in the setup. In our protocol of GM, although R can be chosen freely, we recommend to set a small value of R as the error of the gain G_b is proportional to R (see Eq. (13) in the Appendix).

Let us now consider the possible “cheating” strategies

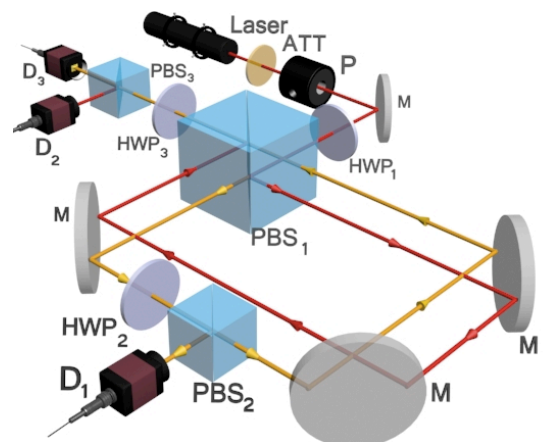


FIG. 2. Experimental demonstration of quantum gambling. ATT represents attenuator which deeply attenuates the laser to the single photon level. P is a polarizer. PBS is the acronym for polarized beam splitter which transmitting horizontal polarized light and reflecting vertical polarized light. HWP indicates the half-wave-plate. HWP₁ is controlled by Alice as the parameter α ; HWP₂ and PBS₂ are inserted in the counter-clockwise route (green line) which are controlled by Bob as the parameter β ; HWP₃ is chosen for projective measurement and acts as the parameter γ . We use three single-photon detectors D₁, D₂, and D₃ to get the three probabilities P_1 , P_2 , and P_3 , respectively. The polarization-Sagnac interferometer ensures a stable system to collect the data.

Alice and Bob might use in this protocol. For Alice, if she prepares the particle not only in boxes A and B but also in another box C, this will only increase the probability of Bob finding the state different from committed state, which has no benefit to Alice herself. Introducing ancillary particles does not help Alice either. So, for Alice, there is no meaningful cheating strategy. However, for Bob, he might try to cheat. He can claim he find the initial state different with the committed state even if

the verification result shows the opposite. Alice cannot tell if Bob is lying or not when the initial state is not the same as the committed state. To detect this cheating, Alice can occasionally prepare the particle in the committed state. However, this detecting procedure will decrease Alice's average gain. To compensate this loss to Alice, the G_a on the Nash-equilibrium point can be set to a value slightly greater than zero. This can be easily achieved by changing γ or R as shown in our protocol.

We note that there are several other quantum protocols [14–17] designed for gambling without third party. However, none of them can achieve a fair game between the casino and the gamblers.

In summary, we have invented a protocol which can promise an unbiased GM to each party by using quantum gambling theory and Nash-equilibrium. Furthermore, the choice of parameter values is flexible, and we have found the relationship between these adjustable parameters, which can be used to guide a feasible implementation of full family of quantum gambling, including both biased and unbiased cases. Compare with related protocols such as quantum coin flipping [6–13] and quantum bit commitment [18–26], the key difference is that quantum gambling makes the cheating as part of strategy, and set flexible rewards to affect the choice of casino and player. This proof-of-principle experiment therefore provides solid support for the applicability and feasibility of our scheme. In a world full of competitions and co-operations, we believe our protocol of gambling machine without a third party will provide direct applications in the near future, and also shed light on developing new quantum technologies.

This work is supported by the Fundamental Research Funds for the Central Universities, National Natural Science Foundation of China (Grant Nos. 11004158, 11374008, 11074198, and 60778021), EPSRC, ERC, QUANTIP, PHORBITECH, and NSQI. J. L. OB. acknowledges a Royal Society Wolfson Merit Award and a Royal Academy of Engineering Chair in Emerging Technologies.

* Xiaoqi.Zhou@bristol.ac.uk

- [1] M. B. Walker, *The psychology of gambling* (Pergamon Press, Oxford and New York, 1992).
- [2] J. F. Nash, Proc. Natl. Acad. Sci. USA **36**, 48-49 (1950).
- [3] D. Meyer, Phys. Rev. Lett. **82**, 1052 (1999).
- [4] J. Eisert, M. Wilkens, and M. Lewenstein, Phys. Rev. Lett. **83**, 3077 (1999).
- [5] For it is a zero-sum game, $G_a = -G_b$, without loss of generality, we can only calculate Bob's average gain G_b .
- [6] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2001).
- [7] R. W. Spekkens and T. Rudolph, Phys. Rev. Lett. **89**, 227901 (2002).
- [8] C. Döschner, and M. Keyl, Fluct. Noise Lett. **2**, R125

- (2002).
- [9] C. Mochon, Phys. Rev. A **72**, 022341 (2005).
- [10] N. Aharon and J. Silman, New J. Phys. **12**, 033027 (2010).
- [11] G. Berlín, G. Brassard, F. Bussi eres, and N. Godbout, Phys. Rev. A **80**, 062321 (2009).
- [12] G. Berl n, G. Brassard, F. Bussi eres, N. Godbout, J. A. Slater, and W. Tittel, Nat. Commun. **2**, 561 (2011).
- [13] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar, Phys. Rev. Lett. **106**, 220501 (2011).
- [14] L. Goldenberg, L. Vaidman, and S. Wiesner, Phys. Rev. Lett. **82**, 3356 (1999).
- [15] P. Zhang, Y.-S. Zhang, Y.-F. Huang, L. Peng, C.-F. Li, and G.-C. Guo, Europhys. Lett. **82**, 30002 (2008).
- [16] W. Y. Hwang, D. Ahn, and S. W. Hwang, Phys. Rev. A **64**, 064302 (2001).
- [17] W. Y. Hwang and K. Matsumoto, Phys. Rev. A **66**, 052311 (2002).
- [18] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
- [19] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
- [20] A. Kitaev, D. Mayers, and J. Preskill, Phys. Rev. A **69**, 052326 (2004).
- [21] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (2007).
- [22] A. Kent, New J. Phys. **13**, 113015 (2011).
- [23] A. Kent, Phys. Rev. Lett. **109**, 130501 (2012).
- [24] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, Nat. Commun. **3**, 1326 (2012).
- [25] J. Kaniewski, M. Tomamichel, E. H nggi, and S. Wehner, IEEE Trans. Inf. Theory **59**, 4687 (2013).
- [26] Y. Liu, Y. Cao, M. Curty, S.-K. Liao, J. Wang, K. Cui, Y.-H. Li, Z.-H. Lin, Q.-C. Sun, D.-D. Li, H.-F. Zhang, Y. Zhao, T.-Y. Chen, C.-Z. Peng, Q. Zhang, A. Cabello, and J.-W. Pan, Phys. Rev. Lett. **112**, 010504 (2014).

APPENDIX

The rules of the protocol can be modified to be general.

The rules of the game: Alice can store a quantum particle in two boxes, A and B , and the state of the particle is denoted by $|a\rangle$ and $|b\rangle$, respectively. However, she only sends one box (suppose box B) to Bob, who will open the box and check where the particle is. Alice and Bob consent to use a superposition state of $|a\rangle$ and $|b\rangle$ as the conventional state. We can define the conventional state to be

$$|\psi_c\rangle = \sqrt{1-\gamma}|a\rangle + \sqrt{\gamma}|b\rangle, \quad (12)$$

Bob wins R coins in one of two cases: finding the particle in box B , or detecting that the state prepared by Alice is different from the conventional state $|\psi_c\rangle$. Otherwise, he loses 1 coin to Alice.

The strategies for them are same as we described in the main text. So the whole game can be acted as this: Alice and Bob choose a state as conventional state $|\psi_c\rangle$ before start. Then Alice chooses a parameter α to prepare a state of Eq. (2), and sends box B to Bob. In Bob's side,

he chooses a splitting parameter β and splits the box B into boxes B and B' . If Bob gets the particle in B , he wins R coins (after Alice check the box A); If B is empty, he asks Alice to send him box A and combines it with box B' to make a verification, then he may win R coins or lose 1 coin depending on the verification results show $|\psi\rangle \neq |\psi_c\rangle$ or $|\psi\rangle = |\psi_c\rangle$, respectively.

Following the rules and the strategies of the game, the expectation value of Bob's gain is

$$G_b = R(P_1 + P_2) - P_3. \quad (13)$$

The state before Bob makes a detection can be written as

$$|\psi_0\rangle = \sqrt{1-\alpha}|a\rangle + \sqrt{\alpha}(\sqrt{1-\beta}|b\rangle + \sqrt{\beta}|b'\rangle). \quad (14)$$

P_1 is the probability of finding particle in box B and it in turn leads to

$$P_1 = \|\langle b|\psi_0\rangle\|^2 = \alpha(1-\beta). \quad (15)$$

The state for verification is

$$|\psi'_0\rangle = \sqrt{\frac{1-\alpha}{1-\alpha+\beta\alpha}}|a\rangle + \sqrt{\frac{\beta\alpha}{1-\alpha+\beta\alpha}}|b'\rangle, \quad (16)$$

while the expecting state to be checked should be

$$|\psi'_c\rangle = \sqrt{\frac{1-\gamma}{1-\gamma+\beta\gamma}}|a\rangle + \sqrt{\frac{\beta\gamma}{1-\gamma+\beta\gamma}}|b'\rangle. \quad (17)$$

If Bob does not find the particle in box B , he will project $|\psi'_o\rangle$ onto $|\psi'_c\rangle$. Then we can get

$$\begin{aligned} P_3 &= (1 - P_1) \|\langle \psi'_c | \psi'_o \rangle\|^2 \\ &= \frac{(\sqrt{(1-\alpha)(1-\gamma)} + \beta\sqrt{\gamma\alpha})^2}{1-\gamma+\beta\gamma}, \end{aligned} \quad (18)$$

$$\begin{aligned} P_2 &= 1 - P_1 - P_3 \\ &= \frac{\beta[\gamma + \alpha - 2\gamma\alpha - 2\sqrt{\gamma\alpha(1-\alpha)(1-\gamma)}]}{1-\gamma+\beta\gamma}. \end{aligned} \quad (19)$$

Substituting Eqs. (6), (9) and (10) into Eq. (4), we can get G_b is in the form of four parameters: α , β , γ and R :

$$G_b = \frac{1}{1-\gamma+\beta\gamma} \{ R(\alpha - \gamma\alpha + \beta\gamma) - (1-\alpha)(1-\gamma) - (1+R)[\beta^2\gamma\alpha - 2\beta\sqrt{\gamma\alpha(1-\alpha)(1-\gamma)}] \} \quad (20)$$

To proof there is a Nash-equilibrium point in the Eq. (20), we use the definition of Nash-equilibrium. In order to find the best strategy for Bob, we should first minimize G_b for α and then maximize the result for β . This means that no matter what strategy Alice chooses, Bob can make sure his gain is no less than a value δ . To find the best strategy for Alice, we should first maximize G_b for β and then minimize the result for α . The calculation yields that the Nash-equilibrium is at

$$\delta = \frac{2+2R-\gamma(2+R)-2(1+R)\sqrt{(1-\gamma)}}{\gamma}; \quad (21)$$

$$\alpha = \frac{1-\sqrt{1-\gamma}}{2}; \quad (22)$$

$$\beta = \frac{-1+\gamma+\sqrt{1-\gamma}}{\gamma}. \quad (23)$$

From Eq. (21), we can know how to choose the parameter of conventional state:

$$\gamma = \frac{4(1+\delta)(1+R)}{(2+\delta+R)^2}. \quad (24)$$

Equations (21), (22), (23), and (24) are the results for general quantum gambling.